UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

MARIA RUSKIEWICZ, on behalf of herself, and all others similarly situated,	)	
Plaintiff	)	
v.	)	**Civil Action File No. 5:23-cv-00303-D**
OKLAHOMA CITY UNIVERSITY,	)	
Defendant	)	

PLAINTIFF'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT OKLAHOMA CITY UNIVERSITY'S MOTION TO DISMISS

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

CASES

Plaintiff MARIA RUSKIEWICZ (hereinafter "Plaintiff"), in opposition to the Motion to Dismiss of the Defendant, OKLAHOMA CITY UNIVERSITY ("Defendant" or "OCU"), respectfully states as follows.

I. INTRODUCTION

This action arises from a data breach to Defendant OCU's systems in July 2022, resulting in the unauthorized disclosure of the Personal Information of its former students and employees—Plaintiff and the proposed Class Members—to cybercriminals. Defendant moves the Court to dismiss Plaintiff's claims for lack of subject matter jurisdiction for lack of Article III standing under Fed. R. Civ. P. 12(b)(1), and to dismiss each of Plaintiff's claims for failure to state a claim upon which relief may be granted under Rule 12(b)(6). For the reasons that follow, OCU's Motion to Dismiss must be denied in whole.

II. FACTUAL AND PROCEDURAL BACKGROUND

Plaintiff is a former student of Defendant and graduate of OCU School of Law. Compl. ¶ 14. On or around July 23, 2022, unauthorized persons infiltrated Defendant OCU's network and gained access to the personal information of approximately 27,229 people, including Plaintiff. *Id.* ¶¶ 3–4. The information accessed included names, addresses, Social Security numbers, driver's license and/or state ID numbers, and passport numbers. *Id.* ¶ 3. Even though Defendant claimed in its notice letter to have discovered the breach immediately, OCU waited over eight months before alerting those affected. *Id.* ¶¶ 7, 43. OCU finally sent Plaintiff and the other affected persons a notice letter dated March 20, 2023. Therein, it urged those affected to "monitor [their] credit reports for suspicious or unauthorized activities" and offered complimentary credit monitoring and identity

protection. *Id.* ¶¶ 7, 40. Plaintiff alleges that the OCU Data Breach occurred as a result of Defendant's failure to implement adequate and reasonable cyber-security procedures and other protocols necessary to protect private information. *Id.* ¶¶ 42. Had Defendant taken reasonable precautions, including training its employees, *Id.* ¶ 51, implementing technical security barriers, *Id.* ¶ 52, abiding by federal regulations *Id.* ¶¶ 53–63, and/or following its own, promised privacy policy, *Id.* ¶¶ 26–29, the breach would not have occurred. *Id.* ¶ 71.

As a result of Defendant's failures to protect Plaintiff's and Class Members' private information and to timely warn Plaintiff and Class Members of the breach, Plaintiff and Class Members have suffered significant injury and damages, including the loss of privacy in their personal information; misuse of their private information; increased spam calls and text messages; delay in receipt of tax refunds; lost time and money spent monitoring financial accounts and protecting against identity fraud; and increased future risk of identity theft. *Id.* ¶ 72. Additionally, because Plaintiff's and Class Members' private information remains stored on Defendant's systems, they have a continuing interest in ensuring that Defendant takes appropriate measures to protect their information against future unauthorized disclosures. *Id.* ¶ 11.

On April 10, 2023, Plaintiff brought this action on behalf of herself and all other "individuals whose Personal Information was compromised as a result of the Data Breach with OCU[,]" *Id.* ¶ 77. In the Complaint, Plaintiff asserted causes of action sounding in negligence (Count I, *Id.* ¶¶ 90–100); negligence *per se*, premised upon OCU's breach of the standard of care in the FTC Act, 15 U.S.C. § 45 (Count II, *Id.* ¶¶ 101–113); breach of express and implied contract (Count III, *Id.* ¶¶ 114–129); unjust enrichment (Count IV, *Id.*

¶¶ 130–136); invasion of privacy (Count V, *Id.* ¶¶ 137–142); and, violation of the Oklahoma Consumer Protection Act, 15 O.S. § 751, *et seq.* (Count VI, *Id.* ¶¶ 143–150). Plaintiff, and the proposed Class, seeks damages and injunctive and declaratory relief.

III. ARGUMENT OF LAW

A. Legal Standard.

Under 12(b)(1), courts may dismiss claims for lack of standing, *Noe v. True*, 2022 U.S. App. LEXIS 27777, *7 (10th Cir.), but "[w]hen considering standing in the context of a motion to dismiss… *must accept* as true all material allegations of the complaint." *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 989 (W.D. Okla. 2021) (emphasis added) (citing *S. Utah Wilderness All. v. Palma*, 707 F.3d 1143, 1152 (10th Cir. 2013)). Moreover, the court "must construe the complaint in favor of the complaining party." *Id*. Under 12(b)(6), courts may dismiss claims for failure to state a claim upon which relief can be granted. But dismissal is improper when a complaint contains "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Kerr v. Polis*, 20 F.4th 686, 700 (10th Cir. 2021) (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). Here, as with Rule 12(b)(6), courts must "take all the plaintiff's well-pleaded facts as true." *Id*. And Rule 8(a)(2) simply requires that complaints provide a "short and plain statement of the claim showing that the pleader is entitled to relief." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)).

B. Plaintiff Has Alleged Sufficient Facts to Demonstrate Article III Standing

1. Article III Standing in Data Breach Caselaw

At the outset, the Court should deny Defendant's Motion to Dismiss under Rule

12(b)(1) for lack of Article III standing. When the well-pleaded facts are taken as true, Plaintiff and the Class have suffered concrete injuries-in-fact, fairly traceable to the Data Breach caused by OCU's tortious conduct. Article III standing "requires a plaintiff to show that [s]he '(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.'" *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 988 (W.D. Okla. 2021) (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016)); *see also, Blood v. Labette Cnty. Med. Ctr.*, No. 522CV04036HLTKGG, 2022 WL 11745549, at *3 (D. Kan. Oct. 20, 2022) (citing *Ward v. Utah*, 321 F.3d 1263, 1266 (10th Cir. 2003) (other citation omitted)). In a "putative class action, the named representative must personally allege that he has standing to sue." *Legg*, 574 F. Supp. 3d at 989; *see Warth v. Seldin*, 422 U.S. 490, 502 (1975); *Big Elk v. Bd. of Cty. Comm'rs of Osage Cty.*, 3 F. App'x 802, 807 (10th Cir. 2001). As this Court recited in *Legg*, to show injury in fact, a plaintiff must allege sufficient facts demonstrating, "that [s]he 'suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id.* (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)). "A 'concrete' injury may include tangible or intangible harms, so long as they 'actually exist' and are "'real,' and not 'abstract.'" *Id.* at 988–89.

As the United States Supreme Court said in *TransUnion LLC v. Ramirez*, looking to *Spokeo, supra:*

> …certain harms readily qualify as concrete injuries under Article III. The most obvious are traditional tangible harms, such as physical harms and monetary harms. If a defendant has caused physical or monetary injury to the

> plaintiff, the plaintiff has suffered a concrete injury in fact under Article III.
>
> Various intangible harms can also be concrete. Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. *Id.*, at 340–341, 136 S.Ct. 1540. Those include, for example, reputational harms, **disclosure of private information**, and intrusion upon seclusion. See, *e.g.*, *Meese v. Keene*, 481 U.S. 465, 473, 107 S.Ct. 1862, 95 L.Ed.2d 415 (1987) (reputational harms); *Davis v. Federal Election Comm'n*, 554 U.S. 724, 733, 128 S.Ct. 2759, 171 L.Ed.2d 737 (2008) (disclosure of private information)...

TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2204 (2021) (emphasis added).”[T]o be ‘imminent,’ a ‘threatened injury must be certainly impending to constitute injury in fact.’” *Blood*, 2022 WL 11745549, at *3 (emphasis added) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013)). “Alternatively, there can be a ‘substantial risk’ that the harm will occur. []But in a suit for damages, the mere risk of future harm—without more—is insufficient to confer standing.” *Blood*, 2022 WL 11745549, at *3 (citing *TransUnion LLC*, 141 S. Ct., at 2210–11).

Because the Tenth Circuit has not yet weighed in on Article III standing in a data breach case, this court in *Legg* examined other Circuit’s rulings on this issue. The court noted that certain courts required allegations that the plaintiff has already experienced fraud or misuse of the personal information (*see Hutton v. Nat’l Bd. Of Examiners in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018) (“The Fourth Circuit similarly found that the plaintiffs had standing to bring claims following a data breach where the plaintiffs alleged that they had ‘already suffered actual harm in the form of identity theft and credit card fraud.’ [but noting that] ‘a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft’”); *Tsao v. Captiva*

MVP Rest. Partners, LLC, 986 F.3d 1332, 1340 (11th Cir. 2021) (same)), whereas other Circuits held that allegations that sensitive personal information was targeted and stolen in a data breach is sufficient to confer Article III standing based on a significant risk of injury (*see Remijas v. Neiman Marcus, LLC*, 794 F.3d 688 (7th Cir. 2015) ("even those plaintiffs who had not experienced fraudulent charges had standing to pursue their claims because their risk of future injury was substantial."); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) ("[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints."); *Attias v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017) (finding standing "because 'a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken.'"); *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010); and *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018) (finding standing based upon imminent risk of identity theft); *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021) (implementing a three-factor test that looks at whether the victims' personal information was targeted in the attach, whether the stolen information was sufficiently sensitive, and whether the stolen information was misused, with not all factors needing to be met).[1]

Federal courts have continued to examine what constitutes injury in fact for Article

[1] The *Legg* court did note that in many Circuits that did not require actual identity theft or fraud for Article III standing, there were named plaintiffs who had in fact suffered fraud or misuse of their stolen information. 574 F. Supp. 3d at 989–91.

III standing purposes in data breach cases. Notably, in *Clemens v. ExecuPharm Inc.*, 48 F.4th 146 (3d Cir. 2022), the Third Circuit Court of Appeals said

> where the asserted theory of injury is a **substantial risk of identity theft or fraud,** a plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, **currently felt concrete harms. For example, if the plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services, the plaintiff has alleged a concrete injury.**

Clemens v. ExecuPharm Inc., 48 F.4th 146, 155–56 (3d Cir. 2022) (emphases added). And, just last month, the Eleventh Circuit Court of Appeals reviewed *TransUnion* and Article III standing in the data breach context in *Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883 (11th Cir. 2023). There, the Court found that the fact that "hackers took credit card data and corresponding personal information from the Chili's restaurant systems and affirmatively posted that information for sale [on the dark web] is the misuse for standing purposes…" *Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 889–90 (11th Cir. 2023). In fact, the Court clarified that this disclosure and posting on the dark web:

> …establishes both a present injury—credit card data and personal information floating around on the dark web—and a substantial risk of future injury—future misuse of personal information associated with the hacked credit card. We hold that this is a concrete injury that is sufficient to establish Article III standing.

Id. at 890. Although this Court is not bound by *Green-Cooper v. Brinker Int'l, Inc.*, it is persuasive as interpreting *TransUnion* and the understanding of "misuse" of unauthorizedly disclosed personal information, as this Court examined in *Legg*.

2. Plaintiff Alleges Ongoing, Imminent, and Increased Harm

Here, Plaintiff has alleged sufficient facts to demonstrate concrete injury for purpose

of establishing Article III standing. This case does not involve some hypothetical risk of future harm, but ongoing and imminent harms, and substantial risk of additional harm, causing currently felt concrete harms. OCU ***admits*** that the Plaintiff's and the Class's personal information was actually "obtained" by cybercriminals during the Data Breach. *See* Compl. ¶ 37; OCU Notice of Data Breach to Plaintiff, March 20, 2023, Compl. Ex. 1. In Defendant's own notice letter, it states that Plaintiff's name address, social security number, driver's license/state ID number, and passport number may have been contained in the personally identifiable information which cybercriminals actually "obtained" in the Data Breach. *See* Compl. Ex. 1. Plaintiff specifically alleged that OCU publicized Plaintiff's and the Class Members' Personal Information to enough people that it is reasonably likely those facts have and/or will become known to the public at large, including, without limitation, on the dark web and elsewhere. *Id.* ¶ 138. As a result, because of this actual disclosure, Plaintiff and the Proposed Class Members allege that their sensitive "Personal Information [has been] **released into the public domain…"**. *See, e.g.*, Compl. ¶¶ 6–7 (emphasis added). Plaintiff alleges that the value of her Personal Information/PII on the black market is considerable, and that criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee, of course. *Id.* ¶ 48.

First, the disclosure of Personal Information itself in the Data Breach is analogous to traditionally recognized harm of disclosure of private information to confer standing. *See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2209 (2021) ("In short, the 1,853 class members whose reports were disseminated to third parties suffered a concrete injury in fact

under Article III."). Next, as in *TransUnion*, and *Green-Cooper v. Brinker Int'l, Inc.*, the fact that Plaintiff alleges that the Personal Information was actually obtained by cybercriminals in the Data Breach, and that cybercriminals post such information to the dark web for sale and criminal fraud constitutes "misuse" for standing purposes. *See* Compl. ¶ 48. Based on the nature of the Data Breach itself in which highly sensitive Personal Information was targeted and stolen, there is a reasonable inference that the cybercriminals are or imminently will use the Personal Information obtained for criminal purposes and identity fraud. *See Galaria*, 663 F. App'x at 388; *McMorris*, 995 F.3d at 1344. This present and imminent misuse distinguishes this case where standing is proper from the Court's decision in *Legg* where it was not.

Second, due to OCU failing to protect the Personal Information disclosed in the Data Breach, Plaintiff and the Class have been required to take measures to deter and detect identity theft and fraud, such as placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports, and accounts for unauthorized activity. *Id*. ¶ 8. They have suffered costs associated with this lost time and effort to mitigate the consequences of the Data Breach, and will be forced to do so into the future. *Id*. ¶ 72. Courts have recognized that mitigation steps like these, when accompanied by the risk of misuse of their stolen information, are sufficient to confer standing. *See Galaria*, 663 F. App'x at 388 ("Where Plaintiffs already know that they have lost control of their data, it would be unreasonable to expect Plaintiffs to wait for actual misuse—a fraudulent charge on a credit card, for example—before taking steps to ensure their own personal and

financial security […] And here, the complaints allege that Plaintiffs and the other putative class members must expend time and money to monitor their credit, check their bank statements, and modify their financial accounts."); *see also, McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 816 (E.D. Ky. 2019) (lost time expended and money due to mitigation efforts to protect their data from misuse constitutes a cognizable injury for Article III standing purposes).

Third, Plaintiff has suffered currently felt harms of embarrassment, humiliation, frustration, and emotional distress by the Data Breach. *Id*. ¶ 99. In *TransUnion*, the Supreme Court elaborated that plaintiffs in this position are "independently harmed by their exposure to the risk itself[.]" *Id*. at 2211; *see also Bowen v. Paxton Media Grp.*, LLC, No. 5:21-CV-00143-GNS, 2022 WL 4110319, at *5 (W.D. Ky. Sept. 8, 2022) (finding standing when plaintiffs "suffered emotional damages related to the breach, which *TransUnion* specifically recognized as a potential concrete injury conferring Article III standing").

Finally, Plaintiff alleges that, as a result of the Data Breach, her Personal Information has diminished in value. *See* Compl. ¶ 72. "Diminution in value of personal information can be a viable theory of damages." *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1234 (D. Nev. 2020), *aff'd*, 845 F. App'x 613 (9th Cir. 2021). Indeed, "[t]he recent set of cases strongly suggest that PII has value." *Hameed-Bolden v. Forever 21 Retail, Inc.*, No. CV 18-03019 SJO (JPRx), 2018 WL 6802818, at *5 (C.D. Cal. Oct. 1, 2018) (collecting cases); *see also In re Facebook Priv. Litig.*, 572 F. App'x 494 (9th Cir. 2014) (recognizing that allegations of diminished value of personal information may be sufficient to establish injury); *In re Marriott Int'l, Inc.*, No. 19-MD-

2879, 2022 U.S. Dist. LEXIS 45764, at *39 (D. Md. Mar. 11, 2022) ("Regardless of whether plaintiffs are pursuing a 'PII Value Damages' theory based on a diminishment in value of their PII or a 'Market Value' theory, Marriott is entitled to obtain discovery to show that these damages theories are not susceptible to classwide proof."). Plaintiff alleges that her Personal Information has value both to herself personally and on the black market. *See* Compl. ¶¶ 48, 72. These allegations suffice at this stage.

As Plaintiff is able to demonstrate Article III standing, OCU's Motion to Dismiss for lack of subject matter jurisdiction under Rule 12(b)(1) should be denied.

3. Plaintiff Has Standing to Pursue Declaratory and Injunctive Relief

In addition, Plaintiff has standing to pursue declaratory and injunctive relief. *See* Compl. ¶¶ 1, 12, 84. Prayer for Relief, D. "'[A] person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *Legg*, 574 F. Supp. 3d at 992–93 quoting *TransUnion*, 141 S. Ct., at 2210 (citing *Clapper*, 568 U.S., at 414, n. 5). Again, Plaintiff and the Class have suffered present and imminent misuse of their Personal Information unauthorizedly disclosed in the Data Breach. This information remains in the hands of OCU, and is subject to further breaches so long as Defendant fails to adequately protect that information. *See* Compl. ¶ 11. Accordingly, Plaintiff and the Class have standing to pursue injunctive relief.

C. Plaintiff Has Sufficiently Pleaded Injury to State a Negligence Claim

Plaintiff adequately argues that OCU's deficient data security practices and protocols allowed unauthorized third-party criminal hackers to enter its data environment,

collect Plaintiffs' PII, remove the PII from its systems, and fraudulently misuse such data. Compl. ¶¶ 2, 3, 5, 6, 10. These allegations are more than sufficient at this stage to establish a plausible connection between the Data Breach and the harms suffered by Plaintiffs and Class members due to the Data Breach. *Id*. ¶¶ 72–76.

As for the loss of time and out-of-pocket costs that follow a Data Breach,"[A] growing number of courts now recognize that individuals may be able to recover Consequential Out of Pocket Expenses that are incurred because of a Breach, including for time spent reviewing one's credit accounts." *In re Anthem, Inc.*, 2016 WL 3029783, at *43 (N.D. Cal. 2016); *see also In re Experian Breach Litig.*, No. SACV151592AGDFMX, 2016 WL 7973595, at *3–5 (C.D. Cal. Dec. 29, 2016); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 403, n.15 (E.D. Va. 2020). *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967–68 (7th Cir. 2016).

With respect to proximate cause in finding negligence under Oklahoma law, the Plaintiff and the Class Members began to incur costs, spent time securing personal accounts, and were at a heightened risk of identity theft only after, and because of, OCU's Data Breach. OCU failed to employ reasonable and appropriate measures against unauthorized access to PII, which constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Compl. ¶¶ 57–58. OCU also failed to train employees on basic cyber security protocols such as detecting phishing emails and other scams, effective passwords management, avoidance of suspicious emails, locking and encrypting files with sensitive information, and implementing guidelines for maintaining sensitive data. *Id*. ¶ 58. OCU's unlawful behavior proximately caused Plaintiff's injuries by failing to maintain

adequate cyber security, failing to implement its privacy policy, failing to adhere to FTC and GLBA standards, failing to protect OCU student and employee PI, failing to monitor its own data security systems, and failing to provide timely notice of the breach. *Id*. ¶ 71.

As a condition of applying for educational purposes or employment, OCU required individuals to provide personal information, and OCU accepted and retained the information. Students and employees were assured that their information would be secured. Given the responsibility of holding and protecting sensitive personal data of tens of thousands of individuals, OCU could or should have foreseen that the Data Breach and the resulting misuse was possible.

The cases cited by the Defendant do not shed light on the highly technical nature of data breaches, the sophistication of modern cybercriminals, or the likelihood of injuries that could plausibly be traced back to a specific data breach. *MBA Commercial Const., Inc v. Roy J. Hannaford Co., Inc.* dealt with a dispute among contractors resulting from construction delays. 818 P.2d 469, 473 (Okla. 1991). As for *Reece v. AES Corporation*, the parties' causation dispute was over the disposal of coal combustion waste and resulting pollution. 638 F. App'x 755, 776 (10th Cir. 2016). Neither illuminate the standard of causation here, and Defendant cites no cases in which time spent and expenses incurred to mitigate against a future risk of identity theft or fraud were found insufficient to satisfy the injury element of a negligence claim. Where, as here, Plaintiffs allege that time was lost and/or expenses were incurred to mitigate the effects of the Breach, the injury element is satisfied. Compl. ¶ 72.

Any specific facts and analysis necessary to support Plaintiffs' allegations that

OCU's negligent data security practices resulted in the Data Breach and, thus, proximately caused Plaintiffs' injuries will continue to be revealed by the parties and supported by expert reports at the appropriate stage of this litigation. OCU's motion to dismiss should be denied.

D. Plaintiff States A Claim For Negligence *Per Se*

Contrary to Defendant's motion, Plaintiff's negligence *per se* claim is both properly pleaded and permitted under the law. Under Oklahoma law, negligence *pe se* allows a plaintiff to "refer to statutory law to show that the defendant owed a duty to the plaintiff." *Armstrong v. Health CARE Serv. Corp.*, 2023 U.S. Dist. LEXIS 10718, at *11 (N.D. Okla.) (citing *Howard v. Zimmer*, 299 P.3d 463, 467 (Okla. 2019)). Moreover, the Oklahoma Supreme Court has explicitly held that "[f]ederal regulations may form the basis of a negligence *per se* claim under Oklahoma law." *Howard v. Zimmer, Inc*., 299 P.3d 463, 467 (Okla. 2013). As such, Section 5 of the FTC Act, which prohibits "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce," 15 U.S.C. § 45(a)(1), can support Plaintiff's negligence *per se* claim. Defendant accuses Plaintiff of portraying the FTC Act's regulations as more concrete than they are, but this argument ignores Plaintiff's allegations about the FCT's own enforcement of its cybersecurity guidelines in the context of Section 5 of the FTC Act. Compl., ¶¶ 54–56; *see also FTC v. Wyndham Worldwide Corp*., 799 F. 3d 236 (3d Cir. 2015) (affirming that the FTC has authority to regulate cybersecurity under Section 5 of the FTC Act).

In fact, courts in the Tenth Circuit readily recognize that violations of Section 5 of the FTC Act can establish negligence *per se* claims. In *Charlie v. Rehoboth McKinley*

Christian Health Care Servs., 598 F. Supp. 3d 1145, 1158, 1167 (D.N.M. 2022), the court refused to dismiss a negligence *per se* claim under the FTC Act, reasoning that Defendant provided "no reason" why the plaintiffs could not allege such a claim and noting that "even though the FTCA provides no private right of action, it may still define the scope of duty that serves as the basis for a negligence *per se* claim." *Id*. And in *Chipotle*, the court held that FTC Act violations may establish negligence *per se* claims when plaintiffs are "consumers, competitors, or otherwise harmed by destruction of competition." *Id*. at 1086. There, the court dismissed the negligence *per se* claim—but only because the plaintiffs were "financial institutions who are neither consumers nor competitors of [the restaurant chain] Chipotle." *Id*. But unlike *Chipotle*, the plaintiff in this case *is* a consumer of Defendant. After all, Plaintiff is a former student of OCU. Compl. ¶ 14. Specifically, Plaintiff paid copious tuition and fees in exchange for Defendant's educational services. *Id*. ¶ 15.[2]

Defendant's arguments in support of a different result are unpersuasive. Most significantly, the cases cited by Defendant do not concern the FTC Act and are factually dissimilar from this case. *Mansfield v. Circle K Corp.*, 877 P.2d 1130 (Okla. 1994), was about local ordinances and state laws that prohibited selling beer to minors. *Smith v. Barker*, 419 P.3d 327 (Okla. Civ. App. 2017), was about a state law that established a right-of-way for pedestrians at crosswalks, and *Alexander v. Smith & Nephew, P.L.C.*, 98 F. Supp. 2d

[2] To the extent Defendant argues that Plaintiff has not sufficiently alleged injury to support her negligence *per se* claim, Plaintiff incorporates by reference her arguments on this topic with respect to the negligence claim.

1310 (N.D. Okla. 2000), and *Howard v. Zimmer, Inc*., 299 P.3d 463 (Okla. 2013), were about defective medical products and the federal Food, Drug, and Cosmetic Act. Simply put, Defendant failed to cite anything on point for its contention that the FTC Act cannot give rise to a negligence *per se* claim in a data breach case. Holding otherwise would be contrary to the wave of case law around the country in data breach actions. Courts have found allegations based on FTC Act and HIPAA violations to be sufficient to support a negligence *per se* claim. *See, e.g., In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, No. 19-MD-2879, 2020 WL 6290670, at *21–23 (D. Md. Oct. 27, 2020) (FTC Act can support a negligence *per se* claim); *In re Equifax, Inc., Customer Data Security Breach Litig.*, 362 F. Supp. 3d 1295, 1327 (N.D. Ga. 2019) (same); *Lamie v. Lendingtree, LLC*, No. 3:22-cv-00307-FDW-DCK, 2023 U.S. Dist. LEXIS 21841, at *9 (W.D.N.C. Feb. 9, 2023) (same). As such, Plaintiff can prevail on a claim sounding in negligence *per se*, and her claim still stands.

E. Plaintiff States a Cause of Action for Breach of Express or Implied Contract

Next, Defendant argues that Plaintiff's claims for breach of express contract and implied contract fail as a matter of law, primarily because OCU argues Plaintiff cannot show the existence of a contract. This argument is without merit. Plaintiff has pleaded sufficient facts to state claim for breach of implied contract, or breach of express contract in the alternative, and OCU's motion to dismiss this count must be denied.

"Under Oklahoma law, in order to recover for breach of contract, [Plaintiff] must establish: '1) formation of a contract; 2) breach of the contract; and 3) damages as a direct result of the breach.'" *Capps v. Bullion Exch., LLC*, No. 18-CV-00162-GKF-FHM, 2019

WL 4918682, at *2 (N.D. Okla. July 9, 2019) (quoting *Dig. Design Grp., Inc. v. Info. Builders, Inc.*, 24 P.3d 834, 843 (Okla. 2001)). "The terms of an express contract are stated in words. The existence and terms of an implied contract are manifested by conduct." *Jones v. Univ. of Cent. Oklahoma*, 1995 OK 138, ¶ 7, 910 P.2d 987, 989 (citing 15 O.S.1991, §§ 131–133). Regardless, "both express contracts and contracts implied in fact are founded on the mutual agreement of the parties." *Erikson v. BP Expl. & Prod. Inc.*, 567 F. App'x 637, 639 (10th Cir. 2014) (quoting *Wattie Wolfe Co. v. Superior Contractors, Inc.*, 417 P.2d 302, 308 (Okla.1966)). "To determine whether an implied contract exists, Oklahoma courts consider various factors, including whether 'one of the parties in good faith has acted in reliance upon the alleged contract.'" *Capps*, 2019 WL 4918682, at *3. "Under *Iqbal's* plausibility standard, [Plaintiff is] required to plead facts that created a *reasonable inference* that there was a contract between [herself] and [Defendant], express or implied, and that [OCU] breached that contract. *Erikson*, 567 F. App'x at 639 (emphasis added) (citation omitted).

First, Plaintiff has pleaded facts sufficient to support a reasonable inference that a contract existed, and that Defendant breached that contract. Plaintiff alleges OCU offered to provide education or employment to Plaintiff and Members of the Class in exchange for payment; that Defendant required them to provide their Personal Information as a condition of that contract. Compl. ¶¶ 115–116. Defendant agreed it would not disclose Personal Information it collects to unauthorized persons, including as stated in its Confidentiality and Privacy Policy, Exhibit 2 ("Privacy Policy"). *See id.* ¶¶ 119. The Privacy Policy explicitly states that:

> As an employee of Oklahoma City University, you may have access to student, employee or other person's academic, personal, health and financial records that may contain individually identifiable information. This information is considered confidential.
> […]
> It is important to handle all confidential information with discretion and it should only be disclosed to others who have a need to know for legitimate business reasons.
> […]
> To safeguard computer data, employees should not share computer login information or leave their computer signed on when away from their desk for extended periods. Computer passwords should be changed regularly. Employees should refer to the University Computer and Network Use Policy for further guidance.

OCU Privacy Policy Ex. 2[3]. Plaintiff clearly identifies contractual obligations on OCU's part for the protection of this data, in maintaining the Privacy Policy and requiring employees to protect student and employee Personal Information per the terms stated therein—including specific data security practices OCU's employees handling data were required to follow, e.g., regularly changing passwords. Moreover, Plaintiff and the Class Members reasonably relied upon OCU's representations to her detriment and would not have provided their sensitive Personal Information to OCU, if not for OCU's explicit and implicit promises to adequately safeguard that information. Compl. ¶ 34. This reliance weighs heavily in favor of the Court finding an implied contract. *See Capps*, 2019 WL 4918682, at *3. The Privacy Policy is no "broad, policy-driven statement[] representing the University's expectations of its staff and its commitment…" but rather the university's policy to maintain student and employee Personal Information *which employees are*

[3] *1.09 Confidentiality And Privacy*, OKLA. CITY UNIV., https://cdn2.assets-servd.host/oklahomacity-university/production/human-resources/docs/Confidentiality-and-privacy.pdf (last accessed Aug. 9, 2023).

required to sign. *Gokool v. Oklahoma City Univ.*, No. CIV-16-807-R, 2016 WL 10520949, at *4 (W.D. Okla. Dec. 29, 2016), *aff'd*, 716 F. App'x 815 (10th Cir. 2017) (citation omitted).

In the alternative, Plaintiff has alleged that OCU's Privacy Policy constitutes an express contract under which Defendant's employees were required to safeguard student and employee Personal Information, including by not sharing login information, not leaving computers unattended, and by changing passwords regularly. It is true that the document is not between Defendant and Plaintiff. However, "[t]he intention of the parties must be ascertained from the four corners of the contract." *Capps*, 2019 WL 4918682, at *3. Here, OCU's promise to students and employees to protect confidentiality of their personal information is readily ascertainable from the Privacy Policy here. Also, "Oklahoma law recognizes that '[a] contract may include a separate writing or portions thereof, if properly incorporated by reference[.]'" *Capps*, 2019 WL 4918682, at *3. OCU's Privacy Policy does not exist in isolation, and discovery will likely reveal numerous other written policies—and agreements with students—concerning the privacy of their information. At this stage, however, Plaintiff has alleged sufficient facts to state a claim for breach of express contract.

Courts routinely refuse to dismiss breach of contract claims in Data Breach cases in connection with privacy policies. *See, e.g. Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1248 (D. Colo. 2018); *Purvis v. Aveanna Healthcare, LLC*, 563 F. Supp. 3d 1360, 1382 (N.D. Ga. 2021); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 485 (D. Md. 2020); *Lochridge v. Quality Temp. Servs., Inc.*,

No. 22-CV-12086, 2023 WL 4303577, at *7 (E.D. Mich. June 30, 2023); *In re Brinker Data Incident Litig.*, No. 3:18-CV-686-J-32MCR, 2020 WL 691848, at *5 (M.D. Fla. Jan. 27, 2020).

Lastly, Plaintiff has adequately alleged that Defendant's breach of its contractual obligations to protect her and the Class Members' Personal Information caused them damages, as set forth in the Complaint. *See* Compl. ¶¶ 123, 129 ("The damages sustained by Plaintiff and Members of the Class as set forth in the preceding paragraphs were the direct and proximate result of Defendant's material breaches of its agreement(s)." Accordingly, Defendant's argument that Plaintiff fails to plead damages caused by OCU's breach of express or implied contract is too without merit.

F. Plaintiff States a Cause of Action for Unjust Enrichment

Under Oklahoma law, unjust enrichment is "[A] condition which results from the failure of a party to make restitution in circumstances where it is inequitable; i.e. the party has money in its hands that, in equity and good conscience, it should not be allowed to retain." *Harvell v. Goodyear Tire & Rubber Co.*, 164 P.3d 1028, 1035 (Okla. 2006).

Here, Plaintiff has pled all the elements necessary to state a claim for unjust enrichment. Plaintiff pled that Defendant "appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and Members of the Class." Compl. ¶ 133. Plaintiff also pled that "Defendant also benefited from the receipt of Plaintiff's and Members of the Class's Personal Information, as this was required to facilitate the student and employment relationship, as well as for the purpose of applying for enrollment or employment." *Id.* Additionally, Plaintiff pled that due to Defendant's conduct, Plaintiff suffered "[A]ctual

damages in an amount equal to the difference in value between the value of their tuition payments or labor with reasonable data privacy and security practices and procedures that Plaintiff and Members of the Class were entitled to, and …[what] they received." *Id.* ¶ 134. Defendant claims that Plaintiff "does not plead facts demonstrating enrichment by OCU or a resulting injustice to her," which is categorically false. Plaintiff was entitled to reasonable data privacy and security practices to protect her PII given that the sensitive disclosure of this information was required to be affiliated with the university. *Id.* ¶¶ 133–135. OCU continues to "retain the monetary value of tuition or labor belonging to Plaintiff and Members of the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself for which Plaintiff and Members of the Class expended tuition or labor and that were otherwise mandated by federal, state, and local laws and industry standards." *Id*. ¶ 135. For Plaintiff to be made whole, Defendant should not be allowed to retain this value for failing to keep promises of data security.

G. Invasion of Privacy—Public Disclosure of Private Fact

Plaintiff sufficiently pleaded a claim for public disclosure of private facts under Oklahoma law. This invasion of privacy tort applies when a defendant (1) publicly discloses (2) private facts (3) highly offensive to a reasonable person and (4) not of legitimate concern to others. *Harris v. Oxbow Carbon LLC*, 2021 U.S. Dist. LEXIS 243600, at *6 (W.D. Okla.) (citing *Hadnot v. Shaw*, 826 P.2d 978, 986 n.30 (Okla. 1992); *Eddy v. Brown*, 715 P.2d 74, 78 (Okla. 1980)). Here, dismissal is improper as Plaintiff's and the Class's PII—which constitutes private facts not of legitimate public concern—were

disclosed to the public (i.e., cybercriminals) via Defendant's Data Breach.

Courts routinely refuse to dismiss such tort claims in data breach cases. *See, e.g.*, *Guy v. Convergent Outsourcing, Inc.*, 2023 U.S. Dist. LEXIS 125332, at *19–20 (W.D. Wash.) (refusing to dismiss the invasion of privacy claim when defendant allegedly "disclosed Plaintiffs' PII by failing to secure it" resulting in a data breach); *Baldwin v. Nat'l W. Life Ins. Co.*, 2021 U.S. Dist. LEXIS 175229 (W.D. Mo.) (refusing to dismiss the invasion of privacy claim when consumer PII was exposed in a data breach). This trend is not surprising because, when a data breach like the one at issue here occurs, the most personal and private information of the plaintiffs is shared with, at a minimum, cybercriminals who have accessed it for the specific purpose of stealing it and selling it on the dark web. *See, e.g.*, Compl. ¶¶ 46, 48, 138. Here, as a result of Defendant's failure to employ reasonable data security practices, Defendant disclosed Plaintiff's PII to, at a minimum, cybercriminals and, almost certainly, to the dark web and the public at large. *Id.* Thus, the Court should decline to dismiss this claim.

In support of its motion, Defendant improperly stretches the holding of the Supreme Court of Oklahoma in *Eddy v. Brown*, 715 P.2d 74 (1986). Although Plaintiff acknowledges *Eddy's* holding that information must be conveyed "to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge," that claim failed only because private information was exposed to "a small group of co-workers." *Id*. at 78. By contrast, in this case, Plaintiff and the Class's PII is now exposed to a staggeringly large number of people via the *world wide web*—an audience far greater than a small group of co-workers. As such, Defendant's motion should

be denied.

H. Plaintiff States a Cause of Action for Violation of the Oklahoma Consumer Protection Act, 15 O.S. §§ 751 *et seq.*

In Count VI of the Complaint, Plaintiff states a cause of action for OCU's violation of the Oklahoma Consumer Protection Act, 15 O.S. §§ 751, *et seq.* ("OCPA"). To prevail on a claim under the OCPA, a plaintiff must demonstrate "(1) that the defendant engaged in an unlawful practice as defined at 15 O.S. (1991), § 753; (2) that the challenged practice occurred in the course of defendant's business; (3) that the plaintiff, as a consumer, suffered an injury in fact; and (4) that the challenged practice caused the plaintiff's injury." *Snider v. Premium Resol. Servs.*, LLC, No. 20-CV-487-JFH-SH, 2022 WL 1836732, at *4 (N.D. Okla. June 3, 2022) (quoting *Patterson v. Beall*, 19 P.3d 839, 846 (Okla. 2000)). "An unlawful practice includes 'a misrepresentation, omission or other practice that has deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person.'" *Id.* (quoting 15 O.S. §§ 752(13); 753(20)). "Because the OCPA is remedial in nature it is to be liberally construed to effectuate its underlying purpose." *Patterson v. Beall*, 19 P.3d 839, 846 (2000 Okla).

Plaintiff has alleged sufficient facts to plausibly state an OCPA claim. She alleges that although OCU alleges it discovered the Data Breach on January 27, 2023, as reported to the Maine Attorney General, OCU's own Notice Letter reported it discovered the Data Breach on July 23, 2022, *and* it failed to notify affected persons in a timely manner until March 20, 2023. Compl. ¶ 43. By failing to promptly, fully and adequately disclose details surrounding the Data Breach, and in its characterizations of the Data Breach in the Notice

letter to Plaintiff and the Class, Defendant OCU utilized deceptive practices in violation of the OCPA. *Id*. ¶¶ 144–47. This is adequate to allege that OCU deceived Plaintiff and the Class Members to their detriment, in its statements regarding the Data Breach and delay in notifying Plaintiff and the Class, to state a violation of the OCPA. OCU does not point to any Oklahoma case refusing to let an OCPA claim in the data breach context proceed at the motion to dismiss stage. Defendant has not met its burden at this stage to show Plaintiff cannot state a plausible claim for relief, and its Rule 12(b)(6) motion must be denied.

I. Injunctive and Declaratory Relief

Finally, Plaintiff sufficiently states a claim for declaratory and injunctive relief. See Compl. ¶¶ 1, 12, 84. Prayer for Relief, D. The standard for a declaratory relief claim is "[W]hether the facts alleged, under all the circumstances, show that there is substantial controversy, between parties having adverse legal interests, of sufficient immediacy and reality to warrant the issuance of a declaratory judgment." *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118, 127 (2007). Additionally, when declaratory relief and injunctive relief appear to be intertwined, that is "yet another reason for refusing dismissal of the request for declaratory relief." *Caspar v. Snyder*, 77 F. Supp. 3d 616, 638 (E.D. Mich. 2015). In *Mackey v. Belden, Inc.*, 2021 WL 3363174 at *12 (E.D. Mo. Aug. 3, 2021), the Court denied the defendant's motion to dismiss the injunctive relief claim, finding that the plaintiff "clearly alleged that her PII remains in [the defendant's] possession and [is] at risk of further disclosure if this Court does not provide injunctive relief."

The declaratory relief standard is met here, as a substantial dispute exists as to what continued risks Plaintiffs and Class members face and, among other things, what specific

security measures Defendant has taken, should take, and whether these measures are any more adequate than they were before the Breach. Additionally, Defendant still possess Plaintiff's PII, and the specific security measures Plaintiff seeks as part of their claim for declaratory and injunctive relief would improve Defendant's data security to prevent future breaches. Compl. ¶¶ 11, 70, 72. Thus, dismissal of the declaratory judgment relief is premature and Plaintiff's claims for injunctive relief and declaratory relief are intertwined.

Here, Plaintiff has pled she suffered and will suffer injury, including the continued risk to her PII which "remains in the possession of OCU and is subject to further breaches so long as it fails to undertake appropriate measures to protect the Personal Information in their possession." *Id*. ¶ 72. The court should follow the reasoning in *Mackey* by denying the dismissal because Plaintiff continues to be at risk of another breach as long as Defendant is in possession of her PII given their questionable security policies and protocols.

Moreover, despite Defendant's assertions otherwise, Plaintiff pled she is at a continued risk of harm that is substantial given the sensitive nature of PII, and the imminent risk of a third-party hacker using the PII to commit fraud or identity theft. *See Id*. ¶¶ 72, 99. Given that a Data Breach from an unauthorized third-party has already occurred, and that Plaintiff's PII is already in the hands of cybercriminals, she is at a continued risk of imminent and substantial harm in the form of identity theft and other financial costs. *Id.*

IV. CONCLUSION

In light of the above, the Motion to Dismiss of Defendant, OKLAHOMA CITY UNIVERSITY should be denied in full.

Dated: August 11, 2023

Respectfully submitted,

/s/ Matthew D. Alison

Jason B. Aamodt, OBA # 16974
Matthew D. Alison, OBA # 32723
INDIAN & ENVIRONMENTAL LAW GROUP, PLLC
233 South Detroit Ave. Suite 200
Tulsa, Oklahoma 74120
(918) 347-6169
jason@iaelaw.com
matthew@iaelaw.com

Lynn A. Toops*
Amina A. Thomas*
Mary Kate Dugan (*Pro Hac Vice* forthcoming)
COHEN &MALAD LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com
mdugan@cohenandmalad.com

J. Gerard Stranch, IV*
Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel Strauss*
Raina Borelli*
TURKE & STRAUSS, LLP
613 Williamson Street Suite 201
Madison, WI 53703
(608) 237-1775
Sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

It is hereby certified that on August 11, 2023 the foregoing MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT OKLAHOMA CITY UNIVERSITY'S MOTION TO DISMISS was filed with the Clerk via the CM/ECF system, which will electronically serve all counsel of record.

/s/ Matthew D. Alison
Matthew D. Alison, OBA # 32723